IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Michael Yip

Serial No.: 09/755,498

Filed: January 5, 2001

For: METHOD AND SYSTEM TO AGGREGATE MULTIPLE VLANs IN A METROPOLITAN AREA NETWORK

Examiner: unassigned

Art Unit: 2152

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner of Patents, Washington, D.C. 20231 on:

February 15, 2002
Date of Deposit

Mark W. Baucher
Name of Person Mailing Correspondence

Signature 2/15/02
Date

Assistant Commissioner for Patents
Washington, D.C. 20231

PETITION TO MAKE SPECIAL FOR PENDING APPLICATION [37 C.F.R. § 1.102(d) / MPEP § 708.2, VIII]

This document is a petition to advance the examination and processing of the above-identified patent application. This petition is submitted pursuant to 37 C.F.R. § 1.102(d) and MPEP § 708.2, VIII.

Advanced examination and processing of the above-identified patent application is respectfully requested per MPEP § 708.2, VIII. Accordingly, the applicants have taken the appropriate steps to comply with the special examining procedures set forth in the MPEP. The steps taken are:

1. This petition to make special has been made with the accompanying fee as set forth in 37 CFR 1.17(i).

2. The claims presented in the above-referenced application are all directed to a single invention.

3. A pre-examination search has been made. A list of the field of search by class and subclass, publication, Chemical Abstracts, foreign patents, and other prior art related material is included below.

4. A copy of each of the references most pertinent to the subject matter encompassed by the claims is attached to this petition, if said references are not otherwise made of record.

5. A detailed discussion of the references, with the particularity required by 37 CFR 1.111(b) and (c), is included in this document. The detailed discussion includes a discussion of how the claimed subject matter is patentable over the references.

PRE-EXAMINATION SEARCH

The following is a list of the field of search by class and subclass, publication, Chemical Abstracts, foreign patents, and other prior art related material:

> 370/218, 370/235, 370/238, 370/239, 370/254, 370/257, 370/279, 370/313, 370/352, 370/355, 370/356, 370/389, 370/392, 370/395, 370/396, 370/401, 370/402, 370/414, 370/466, 375/225, 395/200.54, 455/63, 701/1, 707/9, 707/104, 709/218, 709/219, 709/221, 709/223, 709/224, 709/225, 709/226, 709/227, 709/228, 709/229, 709/238, 709/239, 709/242, 709/243, 709/244, 709/245, 710/129, 713/154, 713/162, 713/168, 713/201, 714/49, and 714/758.

The following primary terms were researched as well:

> networks, local area networks (LANs), virtual LANs (VLANs), VLAN ID, VLAN tag, metropolitan area networks (MANs), virtual MANs (vMANs), routers, bridge, switch, edge switch, protocols, tunneling, aggregation, and derivatives of these terms, e.g. routing instead of router.

The resulting searches provided an extensive list of related patents, none of which was exactly on point, the most pertinent of which are listed below.

U.S. Patent Number	Filing Date	Inventor	Class/Subclass
5,732,078	March 24, 1998	Arrango	370/355
5,737,333	April 7, 1998	Civanlar, et al.	370/395
5,742,604	April 21, 1998	Edsall, et al.	370/401
5,793,763	August 11, 1998	Mayes, et al.	370/389
5,802,106	September 1, 1998	Packer	375/225
5,862,452	January 19, 1999	Cudak, et al.	455/63
5,909,686	June 1, 1999	Muller, et al.	707/104
5,910,955	June 8, 1999	Nishimura, et al.	370/401
5,926,463	July 20, 1999	Ahearn, et al.	370/254
5,938,736	August 17,1999	Muller, et al.	709/243
5,949,783	September 9, 1999	Husak, et al.	370/396
5,978,378	November 2, 1999	Van Seters, et al.	370/401
6,006,258	December 21, 1999	Kalajan	709/219
6,006,264	December 21, 1999	Colby, et al.	709/226
6,006,272	December 21, 1999	Aravamudan, et al.	709/245
6,012,090	January 4, 2000	Chung, et al.	709/219
6,018,619	January 25, 2000	Allard, et al.	395/200.54
6,023,724	February 8, 2000	Bhatia, et al.	709/218
6,028,848	February 22, 2000	Bhatia, et al.	370/257
6,029,203	February 22, 2000	Bhatia, et al.	709/244
6,032,194	February 29, 2000	Gai, et al.	709/239
6,047,325	April 4, 2000	Jain, et al.	709/227
6,049,834	April 11, 2000	Khabardar, et al.	709/242
6,052,803	April 18, 2000	Bhatia, et al.	714/49
6,058,106	May 2, 2000	Cudak, et al.	370/313
6,058,431	May 2, 2000	Srisuresh, et al.	709/245
6,085,238	July 4, 2000	Yuasa, et al.	709/223
6,088,356	July 11, 2000	Hendel, et al.	370/392
6,094,435	July 25, 2000	Hoffman, et al.	370/414
6,094,659	July 25, 2000	Bhatia	707/104
6,098,172	August 1, 2000	Coss, et al.	713/201

6,104,696	August 15, 2000	Kadambi, et al.	370/218
6,104,700	August 15, 2000	Haddock, et al.	370/235
6,105,027	August 15, 2000	Schneider, et al.	707/9
6,108,330	August 22, 2000	Bhatia, et al.	370/352
6,115,378	September 5, 2000	Hendel, et al.	370/392
6,118,768	September 12, 2000	Bhatia, et al.	370/254
6,118,784	September 12, 2000	Tsuchiya, et al.	370/401
6,119,162	September 12, 2000	Li, et al.	709/227
6,119,171	September 12, 2000	Alkhatib	709/245
6,128,657	October 3, 2000	Okanoya	709/224
6,131,163	October 10, 2000	Wiegel	713/201
6,141,749	October 31, 2000	Coss, et al.	713/162
6,151,316	November 21, 2000	Crayford, et al.	370/356
6,154,446	November 28, 2000	Kadambi, et al.	370/239
6,154,775	November 28, 2000	Coss, et al.	709/225
6,154,839	November 28, 2000	Arrow, et al.	713/154
6,157,647	December 5, 2000	Husak	370/401
6,157,955	December 5, 2000	Narad, et al.	709/228
6,167,445	December 26, 2000	Gai, et al.	709/223
6,170,012	January 2, 2001	Coss, et al.	709/229
6,178,455	January 23, 2001	Schutte, et al.	709/228
6,178,505	January 23, 2001	Schneider, et al.	713/168
6,181,681	January 30, 2001	Hiscock, et al.	370/279
6,181,699	January 30, 2001	Crinion, et al.	370/392
6,182,226	January 30, 2001	Reid, et al.	713/201
6,182,228	January 30, 2001	Boden, et al.	713/201
6,188,694	February 13, 2001	Fine, et al.	370/402
6,195,705	February 27, 2001	Leung	709/245
6,202,114	March 13, 2001	Dutt, et al.	710/129
6,208,649	March 27, 2001	Kloth	370/392
6,208,656	March 27,2001	Hrastar, et al.	370/401
6,212,558	April 3, 2001	Antur, et al.	709/221
6,216,167	April 10, 2001	Momirov	709/238
6,219,706	April 17, 2001	Fan, et al.	709/225
6,219,739	April 17, 2001	Dutt, et al.	710/129

6,226,267	May 1, 2001	Spinney, et al.	370/235
6,226,771	May 1, 2001	Hilla, et al.	714/758
6,230,203	May 8, 2001	Koperda, et al.	709/229
6,243,383	June 5, 2001	Li, et al.	370/395
6,243,749	June 5, 2001	Sitaraman, et al.	709/223
6,243,754	June 5, 2001	Guerin, et al.	709/227
6,243,815	June 5, 2001	Antur, et al.	713/201
6,246,669	June 12, 2001	Chevalier, et al.	370/238
6,249,523	June 19, 2001	Hrastar, et al.	370/401
6,252,888	June 26, 2001	Fite, Jr., et al.	370/466
6,253,122	June 26, 2001	Razavi, et al.	701/1
6,256,314	July 3, 2001	Rodrig, et al.	370/401
6,262,976	July 17, 2001	McNamara	370/254
6,266,707	July 24, 2001	Boden, et al.	709/245
6,269,099	July 31, 2001	Borella, et al.	370/389

The publications searched include the following websites:

www.uspto.gov
www.extremenetworks.com
www.cisco.com
www.nortelnetworks.com
www.vipswitch.com
www.3com.com
www.netplane.com
www.cnet.com
www.zdnet.com
www.atrica.com
www.npi.com
www.switchcore.com
internetworking.hitachi.com
www.lucent.com
www.marconi.com
www.netgear.com
www.sun.com
www.enterasys.com
www.altavista.com
www.google.com
www.yahoo.com
www.acm.org
www.ieee802.org
www.ietf.org
www.whatis.com
www.dogpile.com
www.rfc-editor.org
www.novell.com
www.microsoft.com
www.cs.byu.edu
www.cs.fsu.edu
www.networksorcery.com
www.roxen.com
www.intel.com
www.ibm.com
www.hp.com
www.fujitsu.com
www.cabletron.com

Each site was searched for the primary terms above as well as any of the following:

802.1Q, GRE (Generic Routing Encapsulation), ISL (Interswitch Link), WAN (Wide Area Network), encapsulation, 802.3, 802.1p, 802.1u, and 802.1d.

The Pre-Examination search also included an examination of the latest router and LAN switch models offered by the various packet forwarding device vendors, e.g. Cisco Systems, Inc., in order to determine if any new or unknown features may correspond to an invention similar to the one in the above-referenced patent application. Searches through web portals, e.g. www.google.com, also invoked numerous sites that were examined for technology similar to that in the above-referenced patent application.

Other related publications were examined in an attempt to identify computer networking standards similar to the present invention. Those publications are:

B. Kantor, "Internet Protocol Encapsulation of AX.25 Frames," Request for Comments: 1226, May 1991 ("RFC1226").

K. Egevang, "The IP Network Address Translator (NAT)," Request for Comments: 1631, May 1994, ("RFC1631").

W. Simpson, "IP in IP Tunneling," Request for Comments 1853, October 1995, ("RFC1853").

C. Perkins, "IP Encapsulation within IP," Request for Comments 2003, October 1996, ("RFC2003").

K. Hamzeh, et al., "Point-to-Point Tunneling Protocol (PPTP)," Request for Comments 2637, July 1999, ("RFC2637").

D. Farinacci, et al., "Generic Routing Encapsulation (GRE)," Request for Comments 2784, March 2000, ("RFC2784").

Detailed Discussion of Prior Art References

Set forth below are the pending independent claims 1, 12, 18, 19, and 20 of the above-referenced patent.

1. An aggregated virtual local area network (VLAN) architecture system comprising:
a metropolitan area network MAN having at least one of a router and a switch; and
an edge switch connecting the MAN to a super-VLAN, the super-VLAN comprising at least one of a plurality of sub-VLANs, and wherein the edge switch applies a modified bridge forwarding rule to exchange a VLAN ID associated with the sub-VLAN for a VLAN ID associated with the super-VLAN before forwarding a data packet from the sub-VLAN over the MAN using the at least one of a router and a switch.

12. A method of aggregating multiple VLANs in a metropolitan area network comprising:

classifying a data packet originating from a sub-VLAN in accordance with an aggregated VLAN configuration, the aggregated VLAN configuration associating the sub-VLAN with a sub-VLAN ID and a super-VLAN ID;

exchanging the sub-VLAN ID for the super-VLAN ID before forwarding the data packet to a MAN;

classifying a data packet originating from a super-VLAN in accordance with the aggregated VLAN configuration, the aggregated VLAN configuration further associating the super-VLAN with a super-VLAN ID and at least one of a plurality of sub-VLAN IDs; and

exchanging the super-VLAN ID for the at least one sub-VLAN ID before forwarding the data packet to a customer associated with the at least one sub-VLAN ID.

18. An article of manufacture comprising a machine-accessible medium having stored thereon a plurality of instructions for aggregating multiple VLANs in a metropolitan area network, comprising:

classifying a data packet originating from a sub-VLAN in accordance with an aggregated VLAN configuration, the aggregated VLAN configuration associating the sub-VLAN with a sub-VLAN ID and a super-VLAN ID;

classifying a data packet originating from a super-VLAN in accordance with the aggregated VLAN configuration, the aggregated VLAN configuration further associating the super-VLAN with a super-VLAN ID and at least one of a plurality of sub-VLAN IDs;

exchanging the sub-VLAN ID for the super-VLAN ID before forwarding the data packet to a MAN and exchanging the super-VLAN ID for the at least one sub-VLAN ID before forwarding the data packet to a customer associated with the at least one sub-VLAN ID.

19. A method for controlling processing of data packets in a switch connected to a metropolitan area network (MAN), comprising:

propagating a data packet originating from one of a plurality of sub-VLANs, the plurality of sub-VLANs belonging to a super-VLAN;

exchanging a VLAN ID identifying the originating sub-VLAN with a super-VLAN ID identifying the super-VLAN to which the originating sub-VLAN belongs;

controlling the processing of the data packet to the MAN in accordance with the exchanged super-VLAN ID and a destination Media Access Control (MAC) address specified in the data packet.

20. An edge switch for controlling processing of data packets in a metropolitan area network (MAN), comprising:

a port for receiving a data packet on an edge switch originating from one of a plurality of VLANs, the plurality of VLANs associated with a super-VLAN;

a means for assigning a VLAN ID to the data packet that identifies the originating VLAN;

a verifier means for verifying that the assigned VLAN ID matches a value in a memory of the edge switch;

a controller for controlling the processing of the verified data packet to exchange the verified VLAN ID for a super-VLAN ID that identifies the associated super-VLAN; and

a means for propagating the processed data packet to the MAN.

Following is a discussion of the two most relevant prior art patents and each category of prior art references. Independent claims 1, 12, 18, 19, and 20 are patentably distinguishable over each of the prior art references for at least the reasons set forth below.

U.S. Patent Number 5,910,955

U.S. Patent Number 5,910,955, "Switching hub capable of controlling communication quality in LAN," issued to Nishimura, et. al., on Jun. 18, 1999 ("Nishimura") describes a switching hub that implements a VLAN identification tagging technique. The switching hub of Nishimura was designed to maintain communications quality control over a computer network. To do so, the Nishimura switching hub inserts 12-bytes of data into an Ethernet frame between the layer-2 heading and the rest of the data packet. The inserted data is called a VLAN tag. A tagged frame is transmitted/received either within an the switching hub or between two sets of switching hubs. The tagged frame controls communication quality in response to communication content.

When a frame is received on a port within Nishimura switching hub, the hub attaches a LAN number tag to the frame identifying the transmission source. After tagging the frame, the hub places the LAN number in a table within its switch fabric. The frame is then forwarded to another switching hub, where the receiving switch adds port information to the frame. The second edge switch then registers the transmission source LAN number of the received frame,

the transmission source MAC address, and the input port number into a LAN table within its switch fabric.

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is exchanged for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed in Nishimura. Indeed Nishimura teaches away from the claimed subject matter of the present invention because Nishimura determine its routing mechanisms based on a combination of VLAN ID, MAC address, and port information. For example, the switching hub of Nishimura does not exchange the VLAN IDs or other data, but rather adds at least 12 bytes of entirely new header information to a data packet prior to forwarding. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over Nishimura.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reasons. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

U.S. Patent Number 5,978,378

U.S. Patent Number 5,978,378, "Method and apparatus for VLAN support," issued to Van Seters et al. on Nov. 2, 1999 ("Van Seters") describes a device that uses VLAN tags to route data packets over a computer network. The Van Seters device uses logic circuits which examine a received data packet to determine whether the data packet is associated with a particular VLAN. The logic circuits retrieve the following information from each received data packet: the port number on which a packet is received, the protocol type, and (if present) a VLAN tag. The

VLAN tag is examined in order to determine where to transmit the data packet. A predefined table within Van Seters's circuit logic indicates which ports within the bridge/router are associated with a particular VLAN. After the table has been consulted, the frame is only transmitted through ports that have destination devices associated with the VLAN. In conjunction with the VLAN retrieval, the Van Seters device also analyzes layer-3 header information to improve performance.

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is <u>exchanged</u> for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed in Van Seters. Rather, the Van Seters device merely accesses VLAN ID information by examining the 802.1Q tag information already present in the data packet and uses it in conjunction with layer-3 information to determine its routing mechanisms to forward the data packet. Thus Van Seters does not disclose the exchange of VLAN ID data. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over Van Seters.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reasons. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

<u>U.S. Patent Number 5,742, 604</u>

U.S. Patent Number 5,742, 604, "Interswitch link mechanism for connecting high-performance network switches," issued to Edsall et al., in April, 1998 ("Edsall"), describes Interswitch link ("ISL") technology to inter-connect two VLAN-capable Ethernet switches using

the Ethernet media. The packets on the ISL link contain a standard Ethernet frame and VLAN information associated with that frame. A data packet is forwarded only to the switches and interconnected links that have the same ISL address, which controls the flow of broadcasts and transmissions between the switches and routers. Every ISL packet consists of three primary fields: the new ISL header, the original Ethernet frame, and a new checksum appended to the end of the ISL packet.

The header consists of a 40-bit destination address, a 48-bit source address, a 16-bit length field, a 15-bit VLAN ID, and some other miscellaneous information. The ISL VLAN ID is independent of IEEE's 802.1Q VLAN ID and may be used by an edge switch to route a data packet to ISL defined VLANs. Additionally, an ISL packet appends a frame checksum (CRC) to the end of a frame. The CRC is a 32-bit value, which computes a number depending on the length and information contained within a data packet. The ISL header and checksum information add at least 22-bytes of additional information to an Ethernet frame.

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is <u>exchanged</u> for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed in Edsell. Edsell uses encapsulation (see below for a description of encapsulation), adding at least one entirely new header and CRC to a data packet before forwarding the packet. Thus Edsell does not disclose the exchange of VLAN ID data. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over Edsell.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reasons. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

Encapsulation

Encapsulation is commonly used in intranetworking and internetworking environments to facilitate the exchange of data between two network devices. Encapsulation occurs when one data structure is incorporated into another data structure. The encapsulation process takes place in two primary ways. First, encapsulation alters a formatted data packet from one frame type to another. Typically, this is done to overcome changes in media. For example, fragmentation and encapsulation occur when an Ethernet frame is modified so it may be forwarded over from an Ethernet switch to an asynchronous transfer mode ("ATM") backbone. Changing an Ethernet frame into ATM cells require the Ethernet frame to be fragmented into multiple 48-byte segments–called payloads and onto each payload is attached a 5-byte ATM header. The resulting 53-byte cell is then capable of being forwarded an ATM network.

A number of different proposals and standards currently exist for the encapsulation of one protocol over another protocol, documented in various publications. One prior art reference is "Internet Protocol Encapsulation of AX.25 Frames," B. Kantor, Request for Comments: 1226, May 1991 ("RFC1226"). Some forms of encapsulation have even been implemented for transporting a protocol over the same protocol, as documented in prior art reference "IP Encapsulation within IP," C. Perkins, Request for Comments: 2003, Oct. 1996 ("RFC2003").

The second form of encapsulation uses the same principles as described above and plays an integral part in the Open Systems Interconnection ("OSI") networking model. The OSI model defines a networking framework for implementing protocols in seven layers. Starting at top of

the model, control is passed from one layer to the next, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. At each OSI layer additional data is appended to or removed from the front and possibly the tail of a data packet. The appended information may represent statistical, informational, and/or routing data that can be understood at a peer layer at the next station. For example, a layer-3 data packet, such as an IP or IPX data packet, may be encapsulated within a layer-2 frame by adding additional header and trailer information, such as media access control ("MAC") address and Cyclic Redundancy Check ("CRC") information, to the data packet before it is transferred across a network connection. This manner of encapsulation implements protocols, instead of merely changing a data packet from one protocol to another.

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is <u>exchanged</u> for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed by the encapsulation prior art. Rather, the encapsulation prior art adds new data to the data packet and does not exchange data before forwarding the data packet. Thus the encapsulation prior art does not disclose the exchange of VLAN ID data. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over encapsulation.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reasons. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

Tunneling

Tunneling is similar to encapsulation in that one data structure is incorporated into another data structure. However, tunneling differs from encapsulation in that tunneling may insert additional headers between protocols. Examples of prior art references that disclose tunneling include "Tunneling IPX Traffic through IP Networks," D. Provan, Request for Comments: 1234, June 1991 ("RFC1234"), "IP in IP Tunneling," W. Simpson, Request for Comments: 1853, Oct. 1995 ("RFC1853"), and "Point-to-Point Tunneling Protocol (PPTP)," K. Hamzeh, et. al., Request for Comments: 2637, Jul. 1999 ("RFC2637").

RFC1234, which describes IP in IP Tunneling illustrates one example of how the tunneling process works. Specifically, tunneling occurs when an outer IP header is placed in front of an original IP header on a data packet, in a process similar to encapsulation. Other headers may be inserted between the two IP headers, which provides tunnel-specific configuration and routing information.

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is exchanged for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed by the tunneling prior art. Rather, the tunneling prior art adds new data to the data packet and does not exchange data before forwarding the data packet. Thus the encapsulation prior art does not disclose the exchange of VLAN ID data. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over the tunneling.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reasons. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

Network Address Translation

Network Address Translation ("NAT") is an Internet standard that enables a local-area network ("LAN") to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT device, such as a router or server, located at the point where the LAN meets the Internet makes necessary IP address translations. Typically, NAT maps several LAN addresses to one or two internetwork addresses. Often, NAT is incorporated as part of a router and corporate firewall network system. For example, a company may have users who log on to a computer network for local access to company files and databases. Within the LAN a user is assigned an IP address, which identifies the user on the LAN. However, when this same user needs to access information outside the LAN, the company router or firewall maps the local, internal IP address to a global IP address. Global addresses identify the company's network to the world. This mapping process helps ensure security because outgoing or incoming requests must go through a translation process that matches a request/response to a previous request/response. NAT also conserves the number of global IP addresses that a company needs since it allows a company to use a single IP address to communicate with the world.

Various prior art references describe variations and implementations of Network Address Translation ("NAT"), such as "The IP Network Address Translator (NAT)," K. Egevang, Request for Comments: 1631, May 1994 ("RFC1631"), "Method for network address translation," Aravamudan, et. al., U.S. Patent No.6,006,272, Dec. 1999 ("Aravamudan"), and

"Apparatus and methods for routerless layer 3 forwarding in a network," Rodrig, et al., U.S. Patent No. 6,256,314, July 2001 ("Rodrig").

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is exchanged for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed by the NAT prior art. Although NAT does exchange information prior to forwarding the data packet, the information that is exchanged is merely a local IP address for a global IP address, where the local address is a local layer-3 address representing a single network device, and the global address is another layer-3 address representing the same single network device. In claim 1, the VLAN ID associated with a sub-VLAN is exchanged for a VLAN ID associated with a super-VLAN, thereby aggregating numerous VLANs into one super-VLAN. Thus the NAT prior art does not disclose the exchange of VLAN ID data. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over NAT prior art.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reasons. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

GRE

Generic Routing Encapsulation ("GRE") is a proposed standard introduced by the Internet community in an attempt to provide a simple, general purpose mechanism which reduces the problem of encapsulation from its current $O(n^2)$ size to a more manageable size. GRE is documented in "Generic Routing Encapsulation (GRE)," Farinacci, et. al., Request for

Comments: 2784, Mar. 2000 ("RFC2784"). Cisco and other network hardware providers have proposed the standard to provide a generic protocol for interconnecting diverse networks.

GRE encapsulates a payload packet with new and additional header and checksum information. The GRE header includes a Checksum Present bit, Reserved bits, a Version Number field, Protocol Type field, and a Checksum field (RFC2784 provides detailed information on each aspect of the header). The resulting GRE packet is then encapsulated within either the same protocol, or the GRE packet may be encapsulated in a different protocol. For example, an IP packet may first be encapsulated in a GRE packet, adding new header information, then the GRE packet is re-encapsulated into an IPX or IP packet. So, typically, a GRE packet consists of three parts: an outer delivery protocol, a GRE header, and a payload packet.

The primary reason for using GRE is that it makes it possible for two small networks, both with the same subnet, to communicate across a MAN or a WAN more efficiently without using extensive Network Address Translation (NAT).

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is exchanged for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed by the GRE prior art. Rather, the GRE prior art adds new data to the data packet and does not exchange data before forwarding the data packet. Thus the GRE prior art does not disclose the exchange of VLAN ID data. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over the GRE prior art.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reasons. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

802.1Q

A common method of transmitting data packets across a network is known as "frame-tagging." A non-proprietary frame-tagging VLAN communication protocol has been incorporated into the Institute for Electrical and Electronics Engineers (IEEE) 802.1Q standard documented in "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks," IEEE, Dec. 1998. The IEEE 802.1Q standard inserts a VLAN ID into the header between the DataLink header and the frame's user data. The IEEE 802.1Q standard enables packet forwarding devices, such as switches and routers, to determine the VLAN to which a data packet belongs and to forward the packet smoothly to the destination VLAN.

The independent claims 1, 12, 18-20 of the present invention are directed to subject matter in which packets are forwarded based on a single VLAN ID. Specifically each independent claim of the present invention recites the limitation that a VLAN ID associated with the sub-VLAN is exchanged for a VLAN ID associated with a super-VLAN before forwarding the data packet. This limitation is not taught or disclosed by the NAT prior art. This limitation is not taught or disclosed by frame tagging. For example, in the non-proprietary frame tagging described in the IEEE 802.1Q specification a VLAN ID is inserted between the payload and the DataLink header, but no header information is exchanged. By exchanging VLAN IDs, the method of the present invention is capable of extending the system-wide upper limit number of VLANs that can be handled while maintaining complete 802.1Q interoperability. As an example, the IEEE 802.1Q standard dictates that an edge switch can only accommodate 4096

customers, whereas the method of the present invention is capable of accommodating many more customers. For at least this reason, independent claims 1, 12, 18-20 are patentably distinguishable over the frame tagging prior art.

Claims 2-11, 13-17, and 21-24 depend from independent claims 1, 12, 18-20 and should be allowable for the same reason. In addition, the dependent claims recite additional limitations that further distinguish them over the prior art.

Conclusion

For at least the foregoing reasons, Applicants submit that all pending claims 1-24 are in condition for allowance and such action is earnestly solicited.

The applicants therefore respectfully request that this Petition to Make Special be granted and that examination of the present application be advanced to the fullest extent possible.

The petition fee of $130 is included herewith. If there are any additional charges, please charge them to our Deposit Account Number 02-2666. If a telephone conference would facilitate the processing of this petition, the Examiner is invited to contact Donna Jo Coningsby at 503-684-6200.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Dated: 2-15, 2002

Donna Jo Coningsby

Donna Jo Coningsby Reg. No. 41,684

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(503) 684-6200